Cyber Security Requirements for Suppliers

Technical and organizational IT security measures

Supplier shall implement and continuously improve adequate technical and organizational measures following commonly accepted standards to **manage the security of information and IT services and to defend against cyber incidents** (e.g., ISO 27001). Those measures shall satisfy the applicable requirements (depending on the services/products provided) and comprise the following areas *(corresponding ISO 27001:2013 reference in brackets)*:

1. Supplier shall define and maintain a set of policies for information security. *(5.1.1)*
2. Supplier shall define roles and responsibilities for IT security and assign suitable staff. *(6.1.1)*
3. Supplier carries out reasonable background verification on employment candidates in accordance with job role requirements, relevant laws, regulations, and ethics. *(7.1.1)*
4. Supplier's contracts with employees and contractors shall state their responsibilities for security. *(7.1.2)*
5. Supplier's management shall ensure that employees and contractors are aware of and fulfil their information security responsibilities. *(7.2)*
6. Supplier shall identify all organizational assets required for the services and protect them adequately. *(8)*
7. Supplier shall define, document, and implement adequate access control concepts based on business and security requirements, to prevent unauthorized access to Henkel data. *(9.1.1)*
8. Supplier shall ensure that cryptography is used effectively to protect information. *(10.1)*
9. Suppler shall prevent unauthorized physical access, damage, and interference (e.g., environmental threats) to information and information processing facilities required for the services. *(11)*
10. Supplier shall ensure correct and secure operations of information processing facilities and that operations are documented in operating procedures, including change controls, restricting access to operational software, backups & recovery, IT service continuity, capacity management and separation of operational from other IT environments. *(12.1)*
11. Supplier shall protect information and information processing facilities against malware with industry standard measures. *(12.2)*
12. Supplier shall log security events, protect them against tampering, and analyze them to timely detect security incidents. *(12.4.1)*
13. Supplier shall manage technical vulnerabilities, including vulnerability identification (e.g., regular scans, penetration tests), risk assessment, remediation (including patching, hardening, restrictions of software installations etc.). *(12.6)*

14. Supplier shall manage IT networks to protect information in systems and applications (e.g., by firewalls, intrusion preventions systems, network segmentation). *(13.1)*
15. Supplier shall consider information security requirements right from the beginning when acquiring, developing, or enhancing information systems / software (security by design). *(14.1)*
16. If Supplier develops information systems, Supplier shall ensure adequate information security measures within the development lifecycle of information systems / software (e.g., change control procedures, secure coding, testing of security functionality, penetration testing). *(14.2)*
17. Supplier shall establish management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents. *(16.1)*
18. Supplier shall ensure the continuity and security of the contracted services during adverse situations, e.g., a crisis or disaster, by adequate organizational and technical measures. *(17)*
19. Supplier shall ensure that breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements are avoided. *(18.1)*
20. Supplier shall without undue delay inform Henkel on security incidents or breaches affecting services for Henkel, at least by e-mail to infosec@henkel.com. *(16.1 and 18.1)*
21. Supplier shall regularly review its technical and organizational measures to ensure that information security is implemented and operated as expected. *(18.2)*.

Audit rights, independent audit reports and certificates

Supplier shall grant Henkel the rights to **audit and to monitor** the service provision during normal business hours once per year upon reasonable advance notice. Supplier shall provide Henkel with respective information and reasonable assistance to carry out such audit.

Depending on the contracted services, the supplier provides Henkel with independent external audit reports or certificates covering the services, e.g., ISO 27001 or TISAX certificates, SOC 2 Type 2 or ISAE3402 Type II reports

Sub-service providers

Supplier shall only outsource IT services to or share Henkel information with third parties who are bound by written contract to information security requirements. Those information security requirements must not be less protective than the requirements in this document.

Supplier shall regularly monitor, review, and audit the security of IT services they have outsourced (e.g., IT hosting, cloud services).